(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 August 2005 (04.08.2005)

PCT

(10) International Publication Number
WO 2005/069823 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/US2005/001098

(22) International Filing Date: 11 January 2005 (11.01.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/536,776 15 January 2004 (15.01.2004) US

(71) Applicant and
(72) Inventor: SONG, Jun [US/US]; 9 Briarbrook Drive, Briarcliff Manor, NY 10510 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *of inventorship (Rule 4.17(iv)) for US only*

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: CENTRALIZED TRANSACTIONAL SECURITY AUDIT FOR ENTERPRISE SYSTEMS

(57) Abstract: This invention provides a method to achieve centralized security audit for an authentication and authorization and access control system. At the transaction entry point, a transaction ID is created and associated with an audit-request and audit-response object. The entry point can be in a firewall (401), IDS (402), Proxy Server (403), Web Server (404) and Application Server (405). The implementation can be in hardware or software. As the request is passed downstream, a logging event occurring at any desired audit point will be added into the audit-request object during the downstream or audit-response object during the upstream. The accumulated logging event data will then be output to a persistent storage device (203) at the central location, which can be anywhere between the entry point to the end point of the transaction. This request-response based transactional auditing method is then applied to an Identity Management System in order to provide centralized secure audit for authentication, authorization, access control and single sign-on, multi-domain and multi-tiered server systems. Those multi-tiered enterprise systems can include firewall (401), IDS (402), proxy server (403), web server (404), application server (405), Web Services (414), MQ server (406) and mainframe SERVER (407). This audit method can also be applied to pass requests over a system that needs to redirect the requests over multiple external networks such as the Internet.

WO 2005/069823 A2